UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/437,741	05/08/2009	Arunachalam Sundararaman	H0022869/4874/108289	8132

92556   7590   01/23/2017
HONEYWELL/HUSCH
Patent Services
115 Tabor Road
P.O.Box 377
MORRIS PLAINS, NJ 07950

EXAMINER
JASMIN, LYNDA C

ART UNIT	PAPER NUMBER
3629	

NOTIFICATION DATE	DELIVERY MODE
01/23/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentservices-us@honeywell.com
amy.hammer@huschblackwell.com
pto-chi@huschblackwell.com

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

Ex parte ARUNACHALAM SUNDARARAMAN,
CARLOS LOPEZ–REYNA,
and VENKATESH VISWANATHAN

_____

Appeal 2014–006954
Application 12/437,741
Technology Center 3600

_____

Before ANTON W. FETTING, JOSEPH A. FISCHETTI, and
ROBERT J. SILVERMAN, *Administrative Patent Judges.*

FETTING, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE[1]

Arunachalam Sundararaman, Carlos Lopez–Reyna, and Venkatesh
Viswanathan (Appellants) seek review under 35 U.S.C. § 134 of a final
rejection of claims 1–7 and 15–20, the only claims pending in the
application on appeal. We have jurisdiction over the appeal pursuant to
35 U.S.C. § 6(b).

---

[1] Our decision will make reference to the Appellants' Appeal Brief ("Appeal
Br.," filed December 18, 2013) and Reply Brief ("Reply Br.," filed May 28,

The Appellants invented a way of generating security reports. Specification 2:11.

An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below (bracketed matter and some paragraphing added).

> 1. A method of generating reports comprising:
>
> [1] a processor apparatus receiving a sign–in event notification for a process;
>
> [2] a processor apparatus identifying a set of rules
>
> > for controlling the process
> >
> > based upon a source of the sign–in notification,
> >
> > the rules defining
> >
> > > the steps of the process,
> > >
> > > the order in which they occur,
> > >
> > > the number of persons required by the process
> > >
> > > and
> > >
> > > the documentation that is collected into a process report
> > >
> > > > to confirm that the proper steps have been followed;
>
> [3] a processor apparatus receiving a sign–out event notification for the process;
>
> and

2014), and the Examiner's Answer ("Ans.," mailed May 9, 2014), and Final Action ("Final Act.," mailed November 1, 2013).

[4] a processor apparatus associating

a set of images from the area recording portions of the process

with

an event report

in accordance with the identified rules

The Examiner relies upon the following prior art:

Richman US 2003/0206099 A1   Nov. 6, 2003
Rodgers US 2006/0293930 A1   Dec. 28, 2006

Claims 1, 2, 4–7, 15, 16, and 18–20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Richman and Rodgers.

Claims 3 and 17 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Richman, Rodgers, and Official Notice.

ISSUES

The issues of obviousness turn primarily on whether the references applied show it was predictable to identify process control rules based on who signs in or out.

FACTS PERTINENT TO THE ISSUES

The following enumerated Findings of Fact (FF) are believed to be supported by a preponderance of the evidence.

Facts Related to the Prior Art

Richman

01. Richman is directed to a guard-enhancing multiple site integrated security system and method of making same. More particularly, Richman relates to a human security guard oriented system of security service and monitoring. Richman para. 2.

02. Richman describes a security system using video images obtained from cameras relayed to a site control unit equipped with an automated image processor. The images are then relayed to a security system operator who then analyzes the images and informs authorities of an intrusion. Richman para. 14.

03. Richman describes system sensors that communicate any (and all) system event(s) to a checkpoint via a custom protocol. A sensor code identifies the sensor device that transmitted the system event. An event code identifies the actual event and attribute code(s) and value(s) together describe software values for the system event and each individual system event as reported. Each system event can have several attributes. The value of an attribute could be anything from an integer, a string, an image or other data file. Richman para. 64.

04. Each specific site for guard monitoring, and security servicing is first fully analyzed and then evaluated to determine the processes required by the site, and which of these processes can be generalized, and which are necessarily site specific. Richman para. 71.

4

05.   The processes reviewed include logging of sign in and sign out activities. Richman paras. 72–77.

06.   After hours and on weekends, all personnel must sign in and out as well as use the card key for safety reasons. All entries with the card key are recorded in a log file, which identifies the location, time and person using the card. This also allows tracking of the site officer as well. An officer usually patrols the ground level, but will occasionally escort people or check other sites such as the roof. Richman paras. 128–133.

Rodgers

07.   Rodgers is directed to sales call management. Rodgers para. 2.

08.   Rodgers describes available slots being automatically generated for sales calls to be made by sales representatives to sales targets, and reservations for one or more of the available slots being enabled to be made electronically on behalf of one or more sales representatives or entities represented by the sales representatives. Rodgers para. 5.

09.   Rodgers describes a sales force automation system with a computer–based calendar having available time slots. Users specify conditions for generating the available slots. Sign–in lists are delivered electronically to the sales targets based on the slots. The conditions comprise rules and relate to time specified as days or times. The conditions relate to a number of slots per period and to generation of ad hoc slots created in real time. Rodgers para. 6.

10. Rodgers describes rules being applied selectively to sales representations or groups of them who match certain criteria; so that, for example, only representatives with a paid subscription to the reservation service are permitted to reserve certain preferred slots. Rodgers para. 68.

11. Rules can create slots that are pre–reserved for a specific rep. Rodgers para. 69.

12. The reservation tool generates activity reports for staff, group office managers of staff, reps, and sales force management. Rodgers para. 77.

ANALYSIS

The Examiner finds that Rodgers describes a process that defines rules where the rules applied depend on the particular sales representative, identified by signing in. Richman describes assigning rules to security guards that define what site is to be patrolled and how the guard is to patrol the site. The fact that salesmen and security guards both travel around a designated territory and need management and direction to support that travel would motivate one of ordinary skill to adapt the techniques for such management in Rodgers to the context of Richman. Final Act. 3–5.

We are not persuaded by Appellants' argument that

> the claimed "source of a sign-in notification" does not require
> an identifier of any person or group of persons and, instead,
> could be simply a card reader. In contrast, the system of
> Richman is directed to the activities of particular guards and
> Rodgers et al. to particular sales targets.

Appeal Br. 7. The argument is made in the wrong direction. Appellants contend that the claim recites a generic function without any specific implementation and fault the references for actually providing implementation examples for the generic function. A species of a genus anticipates the genus. *Mikus v. Wachtel*, 504 F.2d 1150, 1151 (CCPA 1974); *In re Slayter*, 276 F.2d 408, 411 (CCPA 1960); *In re Gosteli*, 872 F.2d 1008, 10 USPQ2d 1614 (Fed. Cir. 1989).

We are not persuaded by Appellants' argument that "there is no teaching or suggestion whatsoever in Richman or Rodgers et al. of identifying a set of rules based upon a source of the sign-in notification or of associating a set of images with an event report in accordance with the identified rules." Appeal Br. 9. Rodgers explicitly assigns rules based upon the particular representative who is identified by signing in. Thus, the particular set of rules to be applied is identified from the act of signing in to identify the particular representative at hand.

Appellants generally allege that other recited limitations are not found in the references but provide no reasoned analysis. This is insufficient to act as a separate argument under 37 C.F.R. § 41.37. As our reviewing court held,

> we hold that the Board reasonably interpreted Rule 41.37 to require more substantive arguments in an appeal brief than a mere recitation of the claim elements and a naked assertion that the corresponding elements were not found in the prior art.

In re Lovin, 652 F.3d 1349, 1357 (Fed Cir 2011).

As to the limitation of "associating a set of images from the area recording portions of the process with an event report in accordance with the identified rules," the claim does not recite or narrow the manner or

implementation of associating and accordance or the nature or content of an event report. The claim also does not recite or narrow the domain of events reportable in such an event report.

Richman describes a security context in which images of an area are recorded and forwarded for analysis and describes sensors that capture system events and associate such events with images such as these. As any security system necessarily follows the rules of the system, such as the scope of security monitoring, an association between events from the area being monitored is inherently in accordance with rules identified for such monitoring, including those that depend on the particular security guard. The association between the images and event completes the recited association.

We are not persuaded by Appellants' argument that "the problem solved is that of providing an event report that confirms compliance with a set of rules. Since this concept is not recognized, there would be no reason to modify Richman." Appeal Br. 9. The claim does not narrow or recite how a report confirms compliance. As Rodgers describes generating activity reports, such reports would inherently confirm compliance with prospective plans for such activity and accordingly with the rules that created the plans.

More critically, the claim refers to two reports, viz, a process report and an event report. The claim does not recite actually creating the process report, which is the only report recited as having anything to do with compliance. Instead, the claim only recites identifying rules that could be used to identify documentation outside the scope of the claim that could in turn be used to create such a report also outside the scope of the claim. The

8

only report recited as existing, and does not recite how generated, is an event report, which is not recited as having anything to do with compliance. Thus, the argument is also not commensurate with the scope of the claim.

CONCLUSIONS OF LAW

The rejection of claims 1, 2, 4–7, 15, 16, and 18–20 under 35 U.S.C. § 103(a) as unpatentable over Richman and Rodgers is proper.

The rejection of claims 3 and 17 under 35 U.S.C. § 103(a) as unpatentable over Richman, Rodgers, and Official Notice is proper.

DECISION

The rejection of claims 1–7 and 15–20 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2011).

AFFIRMED